# CLAIMS

1. A portable data storage device which can interface with a remote computer such as a desktop PC or a mobile portable notebook computer and which is capable of securing data by reference to a polynomial key generated by pseudo random generated parameters and wherein the device can act as a host or as a client in relation to user access to the data stored therein and wherein the data stored in the device is stored in layered memory architecture and wherein the device is disposed with a communications interface, a microcontroller with a built in switchable input means, a primary and secondary memory storage means, a data processing unit, a data and decision means, a secure key processing unit, an access control decision unit and an encryption smart key storage unit.

2. A device as claimed in claim 1 wherein the communications interface is in two-way communication with the data processing unit.

3. A device as claimed in claim 1 wherein the data processing unit is in communication with the access control decision unit and is in two-way communication with the primary and secondary memory means.

4. A device as claimed in claim 1 wherein the secure key processing unit is reversibly connected with the encrypted smart key storage unit and is further in communication with the access control decision unit.

5. A device as claimed in claim 1 wherein the microcontroller with the built in

switchable input is in communication with the data and decision means.

6. A device as claimed in claim 1 wherein the data and decision means is in communication with the secure key processing unit.

7. A memory storage means as claimed in claim 1 wherein the memory means may be volatile or non volatile and wherein the storage means is capable of reversibly receiving and storing data for multi read/write applications.

8. An access control decision unit as claimed in claim 1 wherein the decision unit determines whether a user may have access to the primary and or the secondary layer memory means in accordance to the user key input.

9. A secure key-processing unit as claimed in claim 1 wherein the secure key-processing unit is responsible for the functionality of encrypting and decrypting key input from users.

10. A data processing unit as claimed in claim 1 wherein the data processing unit processes data stored in the primary and secondary memory means prior to access by the user via the communications interface.

11. A microcontroller unit with built in switchable input as claimed in claim 1 wherein the microcontroller provides a gateway whereby a user may interface with the data storage device via a host computer and wherein the switchable input permits the device to act as a host wherein the device protects access to the data stored in the memory means and permits the

device to as a client wherein the device can be connected to a host computer and wherein the device can permit authorised users to access the computer to which the device is attached.

12. An encrypted smart key storage unit as claimed in claim 1 wherein a factory preset encrypted key is stored.

13. A data and decision means as claimed in claim 1 wherein the data and decision means authenticates the key input from the user and determines whether the user shall be permitted access to the data stored in the primary and or secondary layer memory means.

14. A process of encryption of users key input wherein key input by the user is converted to a pseudo random generated key in accordance with predefined algorithms and wherein this key is combined with the factory preset key in a polynomial sequence appending process to produce a secure key and wherein the secure key is pointed and is only accessible by an encryption pointer key.

15. A process of encryption as claimed in claim 14 above wherein the secure encrypted polynomial key is stored in the memory means.

16. A process of decryption of key input by a user wherein the key input is evaluated and authenticated by the data and decision means and upon authentication an encryption pointer is prepared by key processing unit to retrieve the secure encryption key from the secure memory means and

wherein a secure key is generated by the secure key processing unit in a polynomial sequence appending process wherein the encrypted user key is combined with a factory preset code and wherein this secure key is decrypted by the data processing unit.